# A colleague asks you for advice on why he can't log in to his Gmail account. Looking at his browser, you see he has typed www.gmal.com in the address bar. The screen looks very similar to the Gmail login screen. Your colleague has just fallen victim to what type of attack?

Typo squatting

# A colleague can’t open any Word document he has stored on his local system. When you force open one of the documents to analyze it, you see nothing but seemingly random characters. There’s no visible sign the file is still a Word document. Regardless of what you use to view or open the Word documents, you don’t see anything but random characters. Your colleague was most likely a victim of what type of malware

Virus

Crypto-Malware

RAT

Backdoor

# A colleague has been urging you to download a new animated screensaver he has been using for several weeks. While he is showing you the program, the cursor on his screen moves on its own and a command prompt window opens and quickly closes. You can’t tell what if anything was displayed in that command prompt window. Your colleague says “It’s been doing that for a while, but it’s no big deal.” Based on what you’ve seen, you suspect the animated screensaver is really what type of malware

A Worm

A Trojan

Ransomware

Adware

# A desktop system on your network has been compromised. Despite loading different operating systems using different media on the same desktop, attackers appear to have access to that system every time it is powered up and placed on the network. This could be an example of what type of rootkit

Application

Kernel

Firmware

Virtual

# A disgruntled administrator is fired for negligence at your organization. Thirty days later, your organization's internal file server and backup server crash at exactly the same time. Examining the servers, it appears that critical operating system files were deleted from both systems. If administering those servers during her employment, this is most likely an example of what kind of malware?

Logic bomb

# A piece of malware is infecting the desktops in your organization. Every hour more systems are infected. The infections are happening in different departments and in cases where the users don’t share any files, programs, or even e-mails. What type of malware can cause this type of infection

Virus

RAT

BitLocker

Worm

# A user calls to report a problem with an application you support. The user says when she accidentally pasted an entire paragraph into an input field, the application crashed. You are able to consistently reproduce the results using the same method. What vulnerability might that user have accidentally discovered in that application?

Buffer overflow

# A user in your organization contacts you to see if there's any update to the "account compromise" that happened last week. When you ask him to explain what he means, the user tells you he received a phone call earlier in the week from your department and was asked to verify his userid and password. The user says he gave the caller his userid and password. This user has fallen victim to what specific type of attack?

Vishing

# A user in your organization is having issues with her laptop. Every time she opens a web browser, she sees different pop-ups every few minutes. It doesn't seem to matter which websites are being visited-the pop-ups still appear. What type of malware does this sound like?

Adware

# A user reports seeing "odd certificate warnings" on her web browser this morning whenever she visits Google. Looking at her browser, you see certificate warnings. Looking at the network traffic, you see all HTTP and HTTPS requests from that system are being routed to the same IP regardless of destination. Which of the following attack types are you seeing in this case?

Man-in-the-middle

# A user wants to know if the network is down because she is unable to connect to anything. While troubleshooting, you notice the MAC address for her default gateway setting doesn't match the MAC address of your organization's router. What type of attack has been used against this user?

A. MAC cloning

B. ARP poisoning

C. Disassociation

D. Rogue access point

B. ARP poisoning is an attack that involves sending spoofed ARP or RARP replies to a victim in an attempt to alter the ARP table on the victim's system. If successful, an ARP poisoning attack will replace one of more MAC addresses in the victim's ARP table with the MAC address the attacker supplies in their spoofed responses.

# All of the wireless users on the third floor of your building are reporting issues with the network. Every 15 minutes, their devices disconnect from the network. Within a minute or so they are able to reconnect. What type of attack is most likely underway in this situation?

A. Evil twin

B. Jamming

C. Domain hijacking

D. Disassociation

D. Disassociation attacks against a wireless system are attacks designed to disassociate a host from the wireless access point and from the wireless network. If the attacker has a list of MAC addresses for the wireless devices, they can spoof de-authentication frames, causing the wireless devices to disconnect from the network.

# An employee at your organization is concerned because her ex-spouse “seems to know everything she does.” She tells you her ex keeps accessing her e-mail and social media accounts even after she has changed her passwords multiple times. She is using a laptop at home that was a gift from her ex. Based on what you’ve been told, you suspect the laptop has what type of malware loaded on it

Adware

Keylogger

Logic Bomb

Ransomware

# An organization has both file server and backup server crashed at exactly the same time. By examining the servers, they find that critical operating system files were deleted. What kind of malware the servers were infected?

a. Worm

b. Crypto-malware

c. Trojan

d. Logic bomb

# Attacks by an individual or even a small group of attackers fall into which threat category?

Hactivist

# Attacks by individuals from organized crime are generally considered to fall into which threat category?

Structured threat

# Coming into your office, you overhear a conversation between two security guards. One guard is telling the other she caught several people digging through the trash behind the building early this morning. The security guard says the people claimed to be looking for aluminum cans, but only had a bag of papers—no cans. What type of attack has this security guard witnessed?

Dumpster diving

# Common sources of vulnerability issues for any systems include which of the following?

a. Strong patch management

b. Identity theft

c. Data loss

d. Weak configurations

# Criminal activity on the Internet can include which of the following?

Fraud, extortion, theft, embezzlement, and forgery

# Each time you open a web browser, you see different pop-up ads every few minutes. It doesn't matter which websites are being visited, the pop-ups still appear. What type of attack does this sound like?

a. Ransomware

b. A potentially unwanted program

c. Worm

d. Virus

# Examining the log file of a victim server, you find the cause "Reply from 192.0.0.1: bytes=45000 time<1ms TTL=128". What type of attack has been detected?

a. Integer overflow

b. XSS

c. Buffer overflow

d. SQL injection

# How can proxy servers improve security?

a. They use TLS-based encryption to access all sites

b. They can control which sites and content employees access

c. They enforce appropriate use of company resources

d. They prevent access to phishing sites

# If a hacker has compromised a web application, he may be able to do which of following?

a. Carry out financial fraud

b. Hijack Session Cookies

c. All of the above

d. Steal personal information

# In cross-site scripting, where does the malicious script execute?

a. In the user's browser

b. On a web server

c. None of above

d. On the attacker's system

# Malware engineers sometimes take steps to prevent reverse engineering of their code. A virus, such as Zeus, that uses encryption to resist reverse engineering attempts is what type of malware

Armored Virus

Rootkit

RAT

Crypto-locker

# Malware engineers sometimes take steps to prevent reverse engineering of their code. A virus, such as Zeus, that uses encryption to resist reverse engineering attempts is what type of malware?

Armored virus

# Output encoding and input validation can be considered as mitigation mechanisms for which vulnerability?

a. Cross-site scripting attack

b. All of the above

c. SQL injection

d. Clickjacking

# Several desktops in your organization are displaying a red screen with the message "Your files have been encrypted. Pay 1 bitcoin to recover them." These desktops have most likely been affected by what type of malware?

Ransomware

# To search through a Linux based system to find files containing a phrase, which tool can be used?

a. curl

b. logger

c. chmod

d. grep

# To secure communications during remote access of a system, which tool can be used?

a. SSH

b. dd

c. OpenSSL

d. tcpdump

# Understanding how a hacker attacks will help you can develop a defensive framework by using which of the following?

a. Automated Indicator Sharing

b. Predictive analysis

c. Adversary Tactics, Techniques, and Procedures

d. Threat maps

# Users are reporting that the wireless network on one side of the building is broken. They can connect but can't seem to get to the Internet. While investigating, you notice all of the affected users are connecting to an access point you don't recognize. These users have fallen victim to what type of attack?

A. Rogue AP

B. WPS

C. Bluejacking

D. Disassociation

A. This is a rogue AP attack. Attackers set up their own access points in an attempt to get wireless devices to connect to the rogue APs instead of the authorized access points.

# Users at your organization are complaining about slow systems. Examining several of them, you see that CPU utilization is extremely high and a process called “btmine” is running on each of the affected systems. You also notice each of the affected systems is communicating with an IP address outside your country on UDP port 43232. If you disconnect the network connections on the affected systems, the CPU utilization drops significantly. Based on what you’ve observed, you suspect these systems are infected with what type of malware

Adware

Bot (Botnet)

Cryptolocker

Armored Virus

# Warfare conducted against the information and information processing equipment used by an adversary is known as which of the following?

Information warfare

# Weak configurations can include which of the following?

a. Firmware

b. Open ports

c. Lack of vendor support

d. Use of secure protocols

# Web Penetration can be done by which tool?

a. Burp Suite

b. All the above

c. Whois lookup

d. Nmap

# What does CIA stand for?

Confidence, Integrity, Accountability

Confidentiality, Integrity, Availability

Configuration, Information, Acceptance

Countermeasure, Intrusion, Access

# What is a step of Web Penetration?

a. Information gathering

b. Vulnerability scanning

c. All the above

d. Exploitation

# What is a weakness of the DNS protocol?

a. TCP can be used for large transfers such as zone transfers

b. Its encryption capabilities are slow

c. It is not scalable

d. Requests and replies are sent in plaintext

# What is the best way to ensure that JavaScript cannot be used to access a cookie?

a. Set the HttpOnly flag in the cookie Correct

b. Use non-persistent cookies

c. Do not Set the secure flag in the cookie

d. Use the CAPTCHA system

# What is the most important first step in a penetration test?

a. Collect important information

b. Persistence

c. Reconnaissance

d. Privilege escalation

# What is the name given to a group of hackers who work together for a collectivist effort, typically on behalf of some cause?

Hacktivists

# What is the name given to the group of individuals who not only have the ability to write scripts that exploit vulnerabilities but also are capable of discovering new vulnerabilities?

Elite hackers

# What is the purpose of HTTPS?

a. To enhance communication protocols

b. To implement Single Sign-On

c. To allow enumeration and monitoring of network resources

d. To use SSL or TLS to encrypt a channel over which HTTP traffic is transmitted

# What is the Secure Shell (SSH) protocol?

a. It is an encrypted remote terminal connection program used for remote connections to a server

b. It provides Software as a Service (SaaS)

c. It provides snapshots of physical machines at a point in time

d. It provides dynamic network address translation

# What is the term used to define attacks that are characterized by using tookits to achieve a presence on a target network, with a focus on the long game—maintaining a persistence on the target network?

Advanced persistent threat

# What should you do to address weak configurations?

a. Remove unnecessary apps

b. All of above

c. Change default usernames and passwords

d. Disable unnecessary services

# What term is used to describe the gathering of information from a variety of sources, including non-public sources, to allow an entity to properly focus their defenses against the most likely threat actors?

Threat intelligence

# What term is used to describe the type of threat that is characterized by a much longer period of preparation (years is not uncommon), tremendous financial backing, and a large and organized group of attackers?

Highly structured threat

# What type of attack involves an attacker putting a layer of code between an original device driver and the operating system?

Shimming

# What type of threat exploits system and application vulnerabilities that are unknown to software developers and even anti-malware manufacturers?

a. An on-premises attack

b. A zero-day attack

c. A cloud-based attack

d. A legacy platform attack

# When a hacker captures network traffic and retransmits it at another time, what type of attack is he using?

a. Man in the middle attack

b. Replay attack

c. Bluejacking attack

d. Denial-of-service attack

# When an attacker captures network traffic and retransmits it at a later time, what type of attack are they attempting?

Replay attack

# When discussing threat concerns regarding competitors, which of the following is true?

Where in the past it would take significant risk to copy the detailed engineering specifications of a major process for a firm, today it can be accomplished with a few clicks and a USB drive.

# When you collected important information on the target system, the type of that environment can be changed from \_\_\_\_\_\_ to \_\_\_\_\_\_\_?

a. secure, vulnerable

b. unknown, known

c. unknown, partially known

d. closed, open

# When you update your browser, you get a warning about a plugin not being compatible with the new version. You do not recognize the plugin, and you aren't sure what it does. Why is it important to understand plugins? What attack vector can be involved in plugins?

A. Man in the middle attack

B. Domain hijacking attack

C. Man in the browser attack

D. URL redirection attack

C. Man in the browser attacks are frequently carried out via browser extensions or plugins.

# Whenever you visit Google, you see a certificate warning. Observating the network traffic, you notice that all HTTP and HTTPS requests are being routed to the same IP regardless of destination. What kind of attack are you facing?

a. Evil twin

b. Disassociation

c. Man in the middle

d. MAC cloning

# Which below version is the most secure protocol?

a. TLSv 1.1

b. HTTP

c. SSL

d. TLSv 1.3

# Which is one of the key steps in pentesting and time-consuming?

a. Exploitation

b. Reporting

c. All of above

d. Reconnaissance

# Which of the attacks take advantage of unsanitized file inclusion vulnerability?

a. Remote File Inclusion

b. All the above

c. Local File Inclusion

# Which of the below extensions needs to be blacklisted in file upload areas?

a. .xml

b. .shtml

c. .php

d. All of above

# Which of the following are characteristics of remote-access Trojans

They can be deployed through malware such as worms

They allow attacks to connect to the system remotely

They give attackers the ability to modify files and change settings

All of the above

# Which of the following are most vulnerable to injection attacks?

a. SQL queries based on user input

b. Session ID

c. Network Transport

d. Registry Keys

# Which of the following are not scanned during a vulnerability scan?

a. Network

b. None of above

c. Applications

d. End users

# Which of the following are reasons that the insider threat is considered so dangerous?

Insiders have the access and knowledge necessary to cause immediate damage to an organization; insiders may actually have all the access they need to perpetrate criminal activity such as fraud; and attacks by insiders are often the result of employees who have become disgruntled with their organization and are looking for ways to disrupt operations.

# Which of the following are true concerning attacker skill and sophistication?

Attackers do not have magic skills, but rather the persistence and skill to keep attacking weaknesses; and there is a surprising number of attacks being performed using old attacks, old vulnerabilities, and simple methods that take advantage of "low-hanging fruit."

# Which of the following characteristics of remote-access Trojans?

All of the above:

They can be deployed through malware such as worms; they allow attacks to connect to the system remotely; they give attackers the ability to modify files and change settings

# Which of the following could be an indicator of compromise

Unusual outbound network traffic

Increased number of logins

Large numbers of requests for the same file

All of the above

# Which of the following could be an indicator of compromise?

All of the above:

Unusual outbound network traffic; increased number of logins; large numbers of requests for the same file

# Which of the following is NOT a characteristic of an SQL injection attack?

a. Leave information unaffected

b. Affects code

c. Malicious activity

d. Manipulates database

# Which of the following is the term generally used to refer to the act of deliberately accessing computer systems and networks without authorization?

Attack

# Which of the following is the term used to describe the processes used in the collection of information from public sources?

Open source intelligence

# Which of the following is the term used to refer to individuals who do not have the technical expertise to develop scripts or discover new vulnerabilities in software but who have just enough understanding of computer systems to be able to download and run scripts that others have developed?

Script kiddies

# Which of the following techniques can not be used to prevent SQL injection?

a. Least privilege of database account

b. Parameterized queries

c. All of the above

d. Stored procedures

# Which of these tools is used in penetration testing?

a. Whois Lookup

b. nmap

c. All of above

d. Maltego

# While port scanning your network for unauthorized systems, you notice one of your file servers has TCP port 31337 open. When you connect to the port with netcat, you see a prompt that reads “Enter password for access:”. Your server may be infected with what type of malware

Virus

Cryptolocker

Backdoor

Spyware

# While port scanning your network for unauthorized systems, you notice one of your file servers has TCP port 31337 open. When you connect to the port with netcat, you see a prompt that reads "Enter password for access:". Your server may be infected with what type of malware?

Blackdoor

# While waiting in the lobby of your building for a guest, you notice a man in a red shirt standing close to a locked door with a large box in his hands. He waits for someone else to come along and open the locked door, then proceeds to follow her inside. What type of social engineering attack have you just witnessed?

Tailgating

# You are seeing a bunch of PDFs flood people's inboxes with titles such as "New Tax Rates for 2021." What attack vector is most likely in use?

A. Python

B. Macro

C. Man in the middle

D. DDoS

B. PDFs have macro capability and can execute a variety of code bases if allowed.

# You are testing your systems against weak passwords using the top 100 commonly used passwords. What is this test an example of?

a. Dictionary

b. Rainbow tables

c. Password spraying

d. All are correct

# You are the security administrator for a multinational corporation that has an Active Directory domain. What type of attack uses HTML tags with JavaScript inserted between the <script> and </script> tags?

a. Cross-site forgery attack

b. SQL injection

c. Cross-site scripting

d. Man-in-the-middle

# You are unable to connect to anything. You find that the MAC address for the default gateway setting doesn’t match the MAC address of the router. What kind of attack are you facing?

a. MAC cloning

b. ARP poisoning

c. Rogue access point

d. Disassociation

# You have a helpdesk ticket for a system that is acting strangely. Looking at the system remotely, you see the following in the browser cache: www.micros0ft.com/office. What type of attack are you seeing?

A. PowerShell

B. Domain hijacking

C. URL redirection

D. Disassociation

# You notice some unusual network traffic and discover several systems in your organization are communicating with a rather dubious “market research” company on a regular basis. When you investigate further you discover that users of the affected systems all installed the same piece of freeware. What might be happening on your network

These users unwittingly installed spyware

These systems are all infected with ransomware

This could be normal behavior and nothing to worry about

These systems are infected with logic bombs

# You notice some unusual network traffic and discover several systems in your organization are communicating with a rather dubious "market research" company on a regular basis. When you investigate further you discover that users of the affected systems all installed the same piece of freeware. What might be happening on our network?

These users unwittingly installed spyware

# You notice your PC injected with a malware loaded on startup and also loads a file called netutilities.dll each time Microsoft Word is opened. What kind of attack are you facing?

a. System infection

b. DLL injection

c. Race condition

d. Memory overflow

# Your database server is returning a large dataset to an online user. What kind of attack are you facing?

a. Memory leak

b. LDAP injection

c. Man in the middle

d. SQL injection

# Your desktops is displaying a red screen with the message “Your files have been encrypted. Pay 1 bitcoin to recover them.” Your desktop has most likely been affected by what type of malware?

a. Spraying

b. Crypto-malware

c. Ransomware

d. Spyware

# Your network scan is showing a large number of address changes to the MAC tables and lots of ARP and RARP messages. What is happening?

A. MAC flooding attack

B. Disassociation attack

C. Jamming attack

D. DNS poisoning

# Your organization is struggling to contain a recent outbreak of malware. On some of the PCs, your antivirus solution is able to detect and clean the malware. On other PCs exhibiting the exact same symptoms, your antivirus solution reports the system is “clean.” These PCs are all running the same operating system and same antivirus software. What might be happening

Your firewall rules are allowing attackers to backdoor those PCs

The antivirus solution is reporting false negatives on some of the PC's

The antivirus solution isn’t properly licensed on all systems

Your systems are infected with polymorphic malware

# Your organization's web server was just compromised despite being protected by a firewall and IPS. The web server is fully patched and properly configured according to industry best practices. The IPS logs show no unusual activity, but your network traffic logs show an unusual connection from an IP address belonging to a university. What type of attack is most likely occurring?

Zero day attack

# Your PC is much slower than usual. You see CPU utilization is extremely high and a running process called "btmine" affected the system. You also find that your systems is communicating with an IP address outside your country on UDP port 43232. When you disconnect the network connection, the CPU utilization drops significantly. What type of malware the system infected?

a. Dictionary

b. Hybrid attack

c. Rainbow tables

d. Crypto-malware

# Your scan your network and notice that a large number of address changes to the MAC tables and lots of ARP and RARP messages. What kind of attack are you facing?

a. DNS poisoning

b. Disassociation attack

c. MAC flooding attack

d. Jamming attack

# Your scan your network and notice that a large number of address changes to the MAC tables and lots of ARP and RARP messages. What kind of attack are you facing?

a. MAC flooding attack

b. Disassociation attack

c. Jamming attack

d. DNS poisoning

# Your website is crashing under an extremely high traffic volume. Examining at the traffic logs, you notice tens of thousands of requests for the same URL coming from hundreds of different IP addresses. What kind of attack are you facing?

a. URL redirection

b. Domain hijacking

c. DNS poisoning

d. DDoS

# You're sitting at the airport when your friend gets a message on her phone. In the text is a picture of a duck with the word "Pwnd" as the caption. Your friend doesn't know who sent the message. Your friend is a victim of what type of attack?

A. Snarfing

B. Bluejacking

C. Quacking

D. Collision

# You've been asked to try and crack the password of a disgruntled user who was recently fired. Which of the following could help you crack that password in the least amount of time?

Rainbow tables